AB:MJB

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for the Premises Known and Described as 223 Clove Road, Unit 1, Staten Island, NY 10310 and Any Closed Containers/Items Contained Therein	**TO BE FILED UNDER SEAL** AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT No. 19-MJ1044

I, JOSHUA CROFT, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 223 Clove Road, Unit 1, Staten Island, NY 10310 (the "SUBJECT PREMISES"), further described in Attachment A, for the things described in Attachment B.

2. I have been a Special Agent with the United States Department of Homeland Security Homeland Security Investigations ("HSI") since December 2016. I am currently assigned to the Child Exploitation Investigations Unit, as a part of which I have investigated violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training and daily work related to conducting this type of investigation. As a result of my training and experience in these types of investigations, I am familiar with the techniques and methods of determining whether a child is a minor, the techniques and methods used by individuals to participate in such criminal activity, and the way in which they seek to conceal their activities from detection by law enforcement

authorities. Through my participation in these types of investigations, I have also executed numerous search warrants, including of the searches of premises and electronic devices.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution and proliferation of child pornography.

4. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

DEFINITIONS AND BACKGROUND

5. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct," and "visual depiction" are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "child pornography" is defined in Title 18, United States Code, Section 2256(8), in pertinent part, as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor

engaging in sexually explicit conduct. . . ."[1]

c. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

d. The term "IP Address" or "Internet Protocol Address" means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

e. The term "Internet" refers to a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. The term "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash

[1] See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

memory, CD-ROMs, and other magnetic or optical media.

PROBABLE CAUSE

6. As set forth below, there is probable cause to believe that JAIRO FERREIRA ("FERREIRA") has received and possessed child pornography at the SUBJECT PREMISES.

7. HSI has been conducting an investigation into a website with the Internet address "http://members.new.lp" (the "Website"), which, until recently, served as a platform for the purchase and sale of child pornography. To access the Website, an individual was required to create a unique profile, including a user name and password, and to pay a certain fee to the Website's operator. The Website was recently shut down as a result of HSI's investigation.

8. Pursuant to Mutual Legal Assistance Treaty ("MLAT") requests to Moldova and Ukraine, HSI has obtained customer information from the Website's servers located in Moldova and Ukraine.

9. This customer information shows that FERREIRA used the email account "jay.ferreira@aol.com" ("FERREIRA EMAIL") to create an account with the Website under the username "jafer95021." FERREIRA purchased child pornography on the Website on multiple instances from February 2016 through February 2018.

10. I have reviewed a sample of the files that FERREIRA purchased on the Website from February 2016 through February 2018 and determined that they are, in fact, child pornography. These files, which are available for the Court's review, are described as follows:

a. **"Playtoy Set"** is a file folder containing multiple images of three prepubescent, fully-nude girls (approximately twelve years old) using sex toys on themselves and each other, and performing oral sex on each other.

b. **"m215_(Deli & Sara Gang Bang Video #2)"** is a video file depicting two prepubescent, fully-nude girls (approximately twelve years old) having sex with two adult males.

11. On October 29, 2019 the Honorable Vera M. Scanlon issued an Order requiring Oath, Inc. (the parent company of AOL) to provide records and information associated with the FERREIRA EMAIL. A review of the records from Oath, Inc. revealed that the FERREIRA EMAIL was registered under the name "Jay Ferreira" with a date of birth of April 7, 1985. The date of birth listed on FERREIRA's New York Driver's License and United States Passport is April 7, 1985. The FERREIRA EMAIL account was activated on or about April 13, 2012, and remains active today.

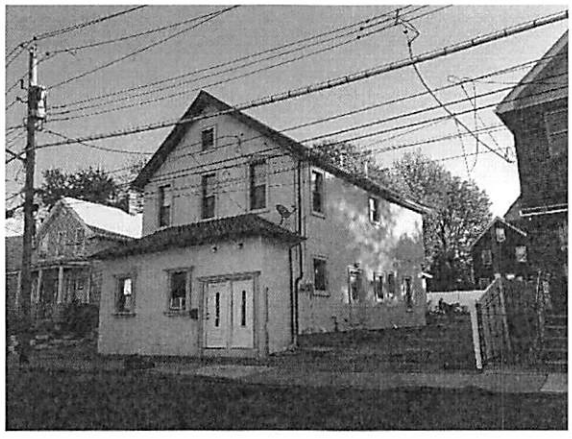
12. Law enforcement recently reviewed records from online food ordering and delivery service companies, Grubhub and Seamless. Grubhub is the parent company of Seamless, and the FERREIRA EMAIL was used in creating an online account. Since March, 2019, approximately 50 food deliveries were made to SUBJECT PREMISES. E-mail alerts and purchase confirmations associated with the approximate 50 food deliveries were sent to the FERREIRA EMAIL.

13. Additionally, a review of New York State Department of Motor Vehicle records reveals that a 2005 Yamaha motorcycle is registered to "FERREIRA, JAIRO M" with a date of birth of April 7, 1985.

14. Finally, I conducted physical surveillance at the SUBJECT PREMISES on November 1 and November 4, 2019, and I observed an individual believed to be FERREIRA enter and exit SUBJECT PREMISES. The individual entering and exiting SUBJECT PREMISES matched the description of the individual pictured on FERREIRA's NY State Driver's License and US Passport.

THE SUBJECT PREMISES

15. The SUBJECT PREMISES is a two unit partially brick house located at 223 Clove Road, Unit 1, Staten Island, NY 10310. The exterior of the SUBJECT PREMISES is pictured below:



16. This search and seizure warrant is specific and limited to all areas within SUBJECT PREMISES that are accessible through the left door. For clarity purposes, left door refers to the door to the left when facing the front exterior of SUBJECT PREMISES from the outside.

17. I have personally seen FERREIRA enter and exit the left door. Based on my investigation thus far, I do not believe FERREIRA utilizes the area accessible from only the right door.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

18. Based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing websites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

19. I know that collectors of child pornography typically retain their materials and related information for many years, in part because it is difficult to obtain and therefore valuable.

20. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

21. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

22. Based on my experience, I know that persons who collect and distribute child pornography frequently collect sexually explicit materials in a variety of

media, such as photographs, magazines, motion pictures, video tapes, books, slides, drawings or other visual media that they use for their own sexual arousal and gratification.

23. Further, based on my training, knowledge, experience and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

TECHNICAL BACKGROUND

24. As described above and in Attachment B, this application seeks permission to search for documents constituting evidence, fruits or instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A that might be found in the SUBJECT PREMISES, in whatever form they are found. One form in which the documents might be found is data stored on a computer's hard drive or other storage media. Thus, the requested warrant would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

25. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, the internal hard drives of computers – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. For example, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

26. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of

the crimes described on the warrant, but also electronic "attribution" evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, Internet search histories, configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data

associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular item is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

27. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. This is true because of the time required for examination, technical requirements and the variety of forms of electronic media, as explained below:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the SUBJECT PREMISES could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify the items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. The variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

28. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques,

including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

29. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

30. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application and search warrant. I believe that sealing these documents is necessary because the investigation into the Website and its customers remains ongoing and, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it might alert the target(s) of the investigation to the existence of an investigation and likely lead to the destruction and concealment of evidence, and/or flight.

Joshua Croft
Special Agent
Homeland Security Investigations

Sworn to before me this
6th day of November, 2019

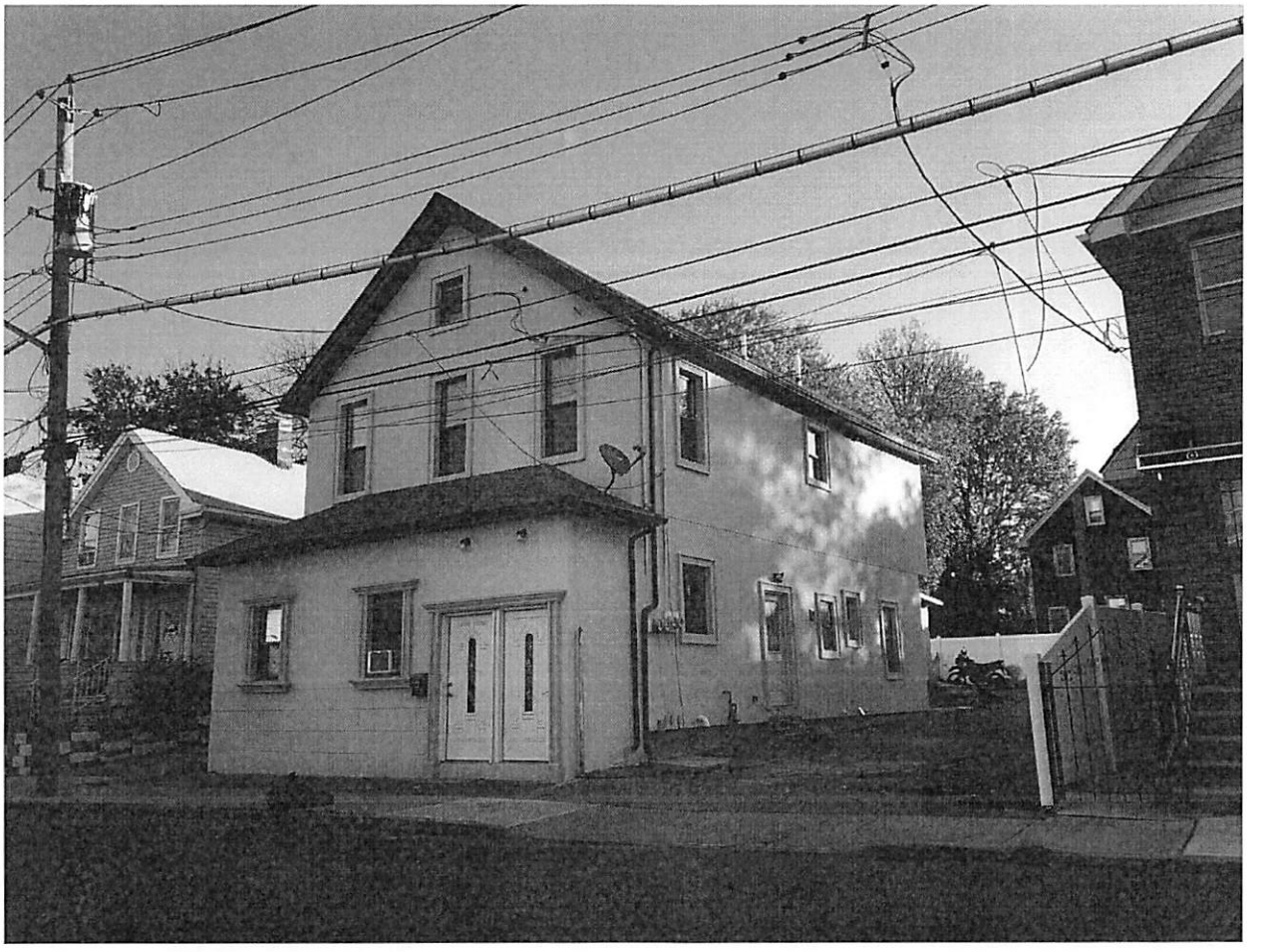
/s/ Scanlon

THE HONORABLE VERA M. SCANLON
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

DESCRIPTION OF THE LOCATION TO BE SEARCHED

The SUBJECT PREMISES is particularly described as 223 Clove Road, Unit 1, Staten Island, NY 10310, specifically all areas accessible through the left door. SUBJECT PREMISES is the two unit partially brick house pictured below:



ATTACHMENT B

DESCRIPTION OF THE PROPERTY TO BE SEIZED

ITEMS TO BE SEIZED FROM THE PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A between January 1 2016 and the present:

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

   a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

   b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including

by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography;

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items;

8. Records evidencing occupancy or ownership of the SUBJECT PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;

9. Records or other items which evidence ownership or use of computer equipment found in the SUBJECT PREMISES, including, but not limited to, sales receipts, bills for Internet access and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct;

11. Address books, names, lists of names and addresses of individuals believed to be minors;

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors;

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors;

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography;

15. Computers[1] or storage media[2] that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

---

[1] A computer includes all types of electronic, magnetic, optical, electrochemical or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers and network hardware, such as wireless routers.

[2] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein, all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.

Any materials seized under this Section that are later determined not to contain or constitute fruits, evidence, and/or instrumentalities of the SUBJECT OFFENSES falling within the categories set forth above will be promptly returned to the SUBJECT PREMISES or to persons reasonably believed to have rightful ownership or custody of the devices.